Privacy Impact Assessments

2008 Data Protection Seminar

TMA Privacy Office

Purpose

- Present an overview of Privacy Impact Assessments (PIAs), to discuss when and why they are completed, to review the basic components, and to discuss their use in Federal Government privacy reporting

Privacy Impact Assessments

Objectives

- This lesson will:
  - Explain PIAs and their importance
  - Locate references on PIAs
  - Identify Privacy reporting requirements
  - Describe how PIAs help safeguard Personally Identifiable Information (PII)

Privacy Impact Assessments

Overview

- What is a PIA?
  - Purpose
  - Goals
- Requirements for PIAs
  - Federal laws, Office of Management and Budget (OMB), Department of Defense (DoD), TRICARE Management Activity (TMA), Service-specific guidance
- PIA roles and responsibilities
  - Preparers, reviewers, signers
- Completing a PIA
- Sources of PIA information

Privacy Impact Assessments

What is a PIA?

- A PIA is an analysis of how PII is handled and protected in an Information Technology (IT) system
- PII is both personal and healthcare information
- Performed at any time within the system lifecycle
- Performed on legacy systems
- PIAs are conducted to:
  - Ensure that systems conform to privacy requirements
  - Assess risks
  - Mitigate potential risks

Privacy Impact Assessments

PIA Goals

- PIAs have four main goals:
  - Internal information
  - Accountability
  - Consistency
  - Remediation
- The PIA must be a stand alone document
- A PIA must be consistent with a system's budget and security documentation

Privacy Impact Assessments

Federal PIA Requirements and DoD PIA

Federal PIA Requirements

- E-Government Act of 2002, Section:
  - Requires agencies to conduct PIAs on IT systems that collect, maintain or disseminate PII about members of the public, or when a system is updated or significantly altered before the development of an IT system (Initiation phase)
- Office of Management and Budget (OMB):
  - OMB M-03-22- OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
  - OMB A-11 Capital Planning Process/Exhibit 300s
  - Federal Information Security Management Act (FISMA)

DoD PIA Requirements

- DoD PIA Guidance Memorandum – October 28, 2005:
  - Issued by DoD Assistant Secretary of Defense (ASD)/Networks Integration and Information (NII)
  - Provided department-wide guidance for implementing the PIA requirements of the E-Government Act
  - Followed OMB Guidance and adds DoD-specific requirements
  - Established questionnaire format of DoD PIAs
- New DoD PIA Policy draft is in final coordination:
  - New DoD PIA Template will be released in conjunction with the new Policy
  - TMA Privacy Office will update all TMA PIA Policy and guidance documents

Privacy Impact Assessments

TMA PIA Guidance and Service-Specific Guid

TMA PIA Guidance

- TMA PIA Guidance Memorandum – February 10, 2006:
  - Delegates PIA compliance responsibilities to the TMA Privacy Officer
  - Includes TMA-specific requirements to address privacy factors
- Directs system owners to:
  - Enter PIA information into the Defense Health Program System Inventory Reporting Tool (DHP SIRT) and DoD Information Technology Portfolio Repository (DITPR)
  - Provide PIA Summary

Service-specific Guidance

- Each Service has their own PIA Guidance:
  - For Service PIAs, TMA will verify and validate information contained in the DHP-SIRT and DITPR, perform a high-level edit, and return comments via email
  - Service PIAs must meet individual service guidelines
  - TMA will acknowledge validation of information via email

Privacy Impact Assessments

PIA Exemptions

- Program Offices will be exempt from PIAs in accordance with OMB Memo 03-22 when:
  - The system is classified as a National Security System (NSS)
  - IT systems do not contain PII
  - All elements of PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act
  - An interagency agreement permitting the merging of data strictly for statistical purposes
  - Another evaluation, as stringent as the PIA process, has been performed [e.g., Data Use Agreement (DUA)]
- In most cases TMA Policy **requires** a PIA Determination Checklist be submitted to the Privacy Office

Privacy Impact Assessments

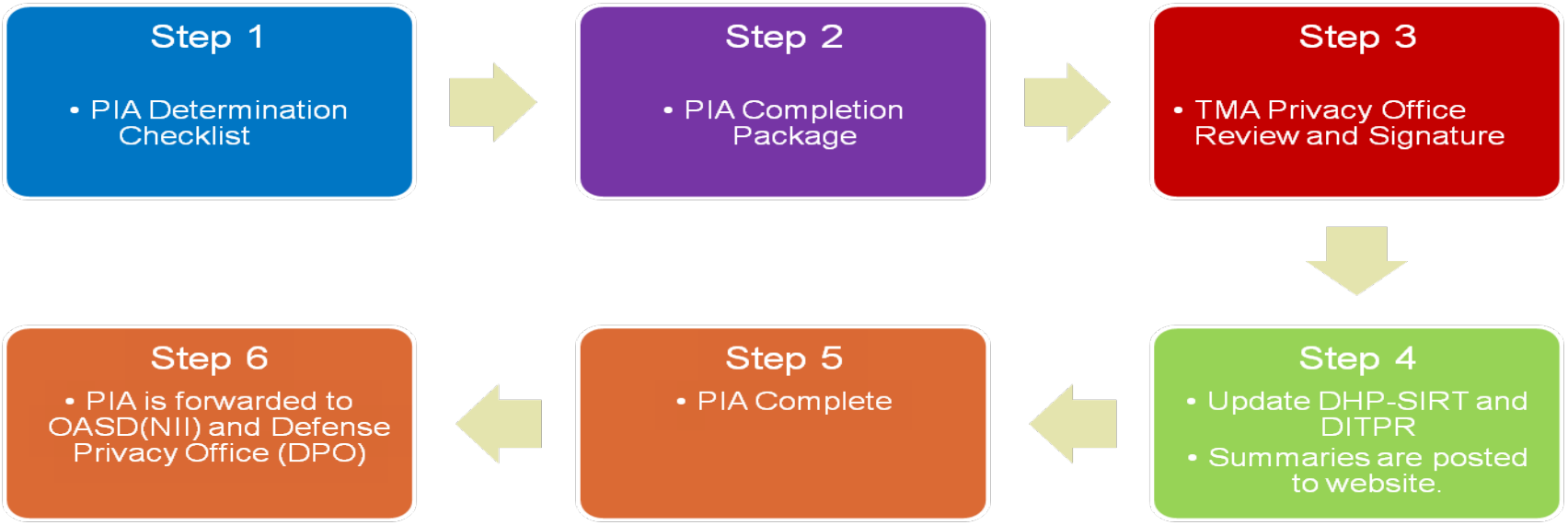
Updating PIAs

- Program Offices must update PIAs or perform new ones when the following conditions occur:
  - Conversion from manual to electronic systems
  - Anonymous to non-anonymous data collections
  - Significant system management changes
  - Significant merging
  - New public access
  - Initiating use of commercial sources
  - New Interagency uses
  - Changes to internal flow or collection
  - Alteration in character of data

Privacy Impact Assessments

PIA Process

- Incorporates Federal and DoD requirements and guidance
- Applies to healthcare service support contractors' systems



Privacy Impact Assessments

Determination Checklist, Determination Evaluation and Complete Package

PIA Determination Checklist

- The PIA determination checklist helps determine if a PIA is required
- This is a TMA Privacy Office assessment tool
- Prior to starting a PIA, the Program Manager completes the checklist and submits it to the Privacy Office
- If a PIA is not needed, the process stops here
- The checklist is kept on file for future reference on how the determination was made

PIA Determination Evaluation

- Key questions:
  - What kind of data does the system use?
  - Does the system contain PII?
  - Is the PII about members of the public?
  - Is the system a National Security system?
  - Have there been major changes to the system?
  - What is the size of the system?

PIA Completion Package

- Documents to assist in preparing a PIA:
  - Service guidance
  - Reference documents:
  - OMB, DoD and TMA PIA guidance
  - DoD and TMA Privacy Office websites

Privacy Impact Assessments

PIA System Information and PIA System Description

PIA System Information

- Defense Health Program (DHP)-funded systems are identified using numbers and names that have been established for purposes other than the PIA submission, including:
  - IT Investment Unique Identifier
  - Budget System Identification Number (IT Registry)
  - System Identification Number (IT Registry)
  - System Points of Contact

PIA System Description

- Key information includes:
  - Issued by DoD Assistant Secretary of Defense (ASD)/Networks Integration and Information (NII)
  - System description - purpose, boundaries, etc
  - System development life cycle Certification and Accreditation (C&A) status
  - A-11 Capital planning exhibits
  - PII maintained in the system
  - Subjects of PII
  - Privacy Act of 1974 compliance

Privacy Impact Assessments

PIA System Description

- Key information includes:
  - System description (purpose, boundaries, etc.)
  - System development life cycle
  - Certification and Accreditation (C&A) status
  - A-11 Capital planning exhibits
  - PII maintained in the system
  - Subjects of PII
  - Privacy Act of 1974 compliance

Privacy Impact Assessments

PIA Information Sharing

- Key points include:
  - Collecting PII from sources other than directly from individuals (databases, websites, etc.)
  - Populating PII for other resources (databases, websites, etc.)
  - Sharing or disclosing PII outside the Service
  - Computer Matching and Privacy Protection Acts
  - Individual choice and notification

Privacy Impact Assessments

PIA Security Controls

- Key resources include:
  - Security control assessments
  - Security plans
  - Contingency plans
  - System and data backup plans
  - Password controls
  - Incident response plans
  - Physical controls (locks, guards, alarms, etc.)
  - Controls on the use of mobile computing devices, removable storage media, remote access

Privacy Impact Assessments

PIA Risk Evaluation

- Evaluates privacy risks
  - Collection, use and sharing of PII
  - Consent and notice for individual data subjects
  - Security controls
- Performed by the Privacy Office during review of completed PIA

Privacy Impact Assessments

PIA Review, PIA Processing, PIA Synopsis

PIA Summary Review

- Signatures may include:
  - Preparing Official- a Government employee
  - Reviewing Officials
  - Chief Privacy Officer (CPO)
  - Chief Information Officer (CIO)
  - Chief Medical Information Officer (CMIO)

PIA Summary Processing

- Signed copies sent to TMA Program Office
- File copy kept in TMA Privacy Office
- TMA Privacy Office validates information in DHP-SIRT and DITPR (all PIAs)
- PIA preparer updates Privacy tab of DHP-SIRT and DITPR (TMA PIAs)
- PIAs are forwarded to OASD(NII) and DPO

PIA Synopsis

- The PIA is a report on the privacy protections in place on an IT system
- PIAs are required for a new system use or maintain PII
- PIAs are required when a system is significantly modified
- Services sign their individual PIAs
- PIA and Privacy information status is reported to OSD through the DHP-SIRT and DITPR
- PIA Information is reported through FISMA Reporting
- TMA goes above and beyond the basic legal requirements

Privacy Impact Assessments

PIA Summary

- You now can:
  - Explain PIAs and their importance
  - Locate references on PIAs
  - Identify Privacy reporting requirements
  - Describe how PIAs help safeguard PII